18th ICCRTS

"C2 in Underdeveloped, Degraded and Denied Operational Environments"

Commercial Technology at the Tactical Edge

Topics:
(7): Architectures, Technologies, and Tools
(8): Networks and Networking

Jonathan R. Agre
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311, USA
+1-703-933-6522
jagre@ida.org

Karen D. Gordon
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311, USA
+1-703-845-2343
kgordon@ida.org

Marius S. Vassiliou
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311, USA
+1-703-887-8189
+1-703-845-4385
mvassili@ida.org

Point of Contact:

Marius S. Vassiliou
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311
USA
+1-703-887-8189
+1-703-845-4385
mvassili@ida.org

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **JUN 2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2013**
4. TITLE AND SUBTITLE **Commercial Technology at the Tactical Edge**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Institute for Defense Analyses,4850 Mark Center Drive,Alexandria,VA,22311**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 18th International Command & Control Research & Technology Symposium (ICCRTS) held 19-21 June, 2013 in Alexandria, VA. U.S. Government or Federal Rights License

14. ABSTRACT
The use of commercial Information and Communications Technology (ICT) at the tactical edge is increasing for many reasons, including commercial ICT?s advanced capabilities, faster time to deployment, and lower cost. One example is the use of smartphones and other handheld computing platforms in military environments. The U.S. Department of Defense has experimented extensively with such devices at the tactical edge, and has also examined the use of commercial smartphones for more general military-grade secure communications. Current efforts to apply such devices and technologies for the warfighter entail both benefits and limitations, with cheap processing and communications capability often trading off against robustness and security. The variety of applications available in the consumer market for smartphones and tablets represent a tremendous base from which the military can draw. However, the fast pace of commercial product cycles requires any customization to be carefully considered and properly architected. A number of emerging applications from the commercial world are identified that could be used more routinely at the tactical edge in the near future. These include software defined networking, autonomous networks, cognitive radios, and methods for hands-free operation. There are many impediments to the effective adoption of commercial ICT at the tactical edge. Some stem from unique technical challenges associated with the rigors of the military environment, while others are primarily organizational and bureaucratic.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**40**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Abstract

The use of commercial Information and Communications Technology (ICT) at the tactical edge is increasing for many reasons, including commercial ICT's advanced capabilities, faster time to deployment, and lower cost. One example is the use of smartphones and other handheld computing platforms in military environments. The U.S. Department of Defense has experimented extensively with such devices at the tactical edge, and has also examined the use of commercial smartphones for more general military-grade secure communications. Current efforts to apply such devices and technologies for the warfighter entail both benefits and limitations, with cheap processing and communications capability often trading off against robustness and security. The variety of applications available in the consumer market for smartphones and tablets represent a tremendous base from which the military can draw. However, the fast pace of commercial product cycles requires any customization to be carefully considered and properly architected. A number of emerging applications from the commercial world are identified that could be used more routinely at the tactical edge in the near future. These include software defined networking, autonomous networks, cognitive radios, and methods for hands-free operation. There are many impediments to the effective adoption of commercial ICT at the tactical edge. Some stem from unique technical challenges associated with the rigors of the military environment, while others are primarily organizational and bureaucratic.

1 Introduction

The recently published *Capstone Concept for Joint Operations* (CCJO) advocates *globally integrated operations* as the foundational concept upon which future Joint Forces operations should be based. A key element of globally integrated operations is *mission command*, a command philosophy characterized by decentralization and empowered by advances in *information and communications technology* (ICT) and mobility computing.[1]

> *Mobile devices with reach-back to network-based services will allow distributed commanders and staffs to collaborate as though co-located. Developing networks that can simultaneously integrate secure and non-secure communications will widen the circle of actors who can support a given operation, allowing diverse stakeholders to contribute insights and expertise in real time.*

The commercial sector has made tremendous advances in ICT and mobility computing in the past decade, spawning innovations such as smart phones, tablets, app stores, and new generations of cellular networks. Due to the initiatives of individual soldiers, commercial devices on the front lines are already a reality. It is imperative that the DoD, as an enterprise, leverage these innovations both to gain capabilities and to save money. Some of the advantages of adopting Commercial-Off-the-Shelf (COTS) technologies include: 1) advanced features (e.g., processing power, memory, communication media, communication speeds, GPS, video cameras, USB) and functions (e.g., apps, chat, maps), 2) faster time to market, 3) less cost, 4) less R&D for the government, and 5) reduced size, weight, and power compared with similar military systems.

The limitations to commercial adoption primarily arise due to the special requirements of the warfighters at the tactical edge and involve technical, environmental, policy and acquisition considerations. Typical environmental examples are survivability in the face of hostile action, lack of fixed infrastructure, high mobility and ruggedness. Technical issues include robustness (in the face of loss of signals) and security. Acquisition impediments arise from the myriad regulations and processes involved with DoD procurement.

The direct adoption of commercial off the shelf (COTS capabilities without modification is typically not a viable practice for use at the tactical edge. Rather, modification of COTS product by the original developers or by third-party vendors to meet the military requirements is increasingly common. However, a desirable goal is to modify COTS device in a modular fashion so that there is the ability to evolve with the market-driven commercial evolution of the device.

In this paper, we begin by identifying some of the major trends driving the use of commercial ICT at the tactical edge. Then we will examine the challenges faced by employing ICT at the tactical edge, explore examples of what the military is doing to incorporate commercial ICT, identify other opportunities for possible exploitation of commercial technologies, and lastly point out some potential areas that are emerging but in which further science and technology research is needed.

---

[1] Joint Chiefs of Staff, *Capstone Concept for Joint Operations (CCJO): Joint Force 2020*, Sept. 10, 2012, http://www.dtic.mil/futurejointwarfare/concepts/ccjo_2012.pdf.

2 Technology, Policy, and Acquisition Trends

There are major trends motivating the DoD to leverage commercial ICT at the tactical edge, some that have existed for many years and others that have emerged more recently:

- Declining influence of DoD on the ICT sector. DoD represents only a small segment of the ICT market and thus has limited influence on the industry. This has been recognized—and acknowledged to some extent by the DoD, as demonstrated by its move to open standards, commercial off-the-shelf (COTS) products, and open source software solutions—for a long time. For example, a 1999 RAND study reported the decline, noting, "The U.S. military market now makes up just 2 percent of the demand for information technology in the United States, down from 25 percent in 1975."[2]
- Consumerization of ICT. Soldiers at the edge now expect wireless capabilities that are comparable to their experiences with their personal devices with connectivity to their lateral, subordinate, and superior commanders, as well as to the Internet and the world-wide cellular networks. In addition, they expect a variety of military and other applications to be available for download and use.

  Senior military leaders concur that soldiers should have access to today's ICT technology. For example, in 2008, General James Cartwright, then the Vice Chairman of the Joint Chiefs of Staff, issued a memorandum advocating the use of commercially-based tools for the transfer of most official information, including military operation orders, stating, "The tools currently available for use include wikis, blogs, chat, and individual e-mail using public key infrastructure certificates."[3]

  More recently, General Keith Alexander, Director of the National Security Agency advocated an app store for the DoD and the Intelligence Community, saying, "What we have to do is create apps for the cloud, put them up there, verify that the apps work as intended, and then let the analysts and people choose the apps that they want."[4]
- Growing demand for cybersecurity solutions. DoD is no longer alone in demanding cybersecurity solutions. As the nation's critical infrastructure sectors – which include banking and finance, energy, transportation, emergency services, health care and public health, and water[5] – become increasingly dependent on ICT, a wider range of commercially-based cybersecurity solutions are becoming available. In addition, individuals and corporations of all sizes—many aspects of whose lives and businesses are maintained online— are demanding cybersecurity solutions to protect their privacy and livelihoods.

---

[2] Z. Khalilzad, et al., *Strategic Appraisal: The Changing Role of Information in Warfare*, RAND Corporation, 1999, http://www.rand.org/pubs/monograph_reports/MR1016.

[3] CM 20005-08, "Use of Defense Message System (DMS) for Official Information (OI)," Memorandum From General James E. Cartwright, Vice Chairman of the Joint Chiefs of Staff, 26 November 2008.

[4] T. Costlow, "NGA apps for GEOINT facilitate mobile, tactical tools," *Defense Systems*, 15 January 2013, http://defensesystems.com/articles/2013/01/15/c4isr-1-geoint-apps.aspx.

[5] Department of Homeland Security, *National Infrastructure Protection Plan (NIPP)*, 2009, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

- Tradeoffs among competing requirements, for example, urgency of information exchange and security. In a 2009 interview, LTG Jeffrey Sorenson, then the Army CIO/G-6, acknowledged that sometimes it makes sense to trade stringent security requirements for timeliness. He said, "In some cases, the financial industry has built a capable system for encryption that we in the Army could leverage — giving us enough security to satisfy what Soldiers need on the battlefield but not restricting our ability to deliver the network. We have examples in theater where Soldiers say the information presented in the forefront of the battlefield is cutting edge and very critical information, but within a few minutes, it becomes historical information. Therefore, why can't we make sure that we get everybody that situational awareness and maybe, in some cases, take a little risk because within a few minutes it is going to become obsolete anyway?"[6]
- DoD telework policy. The DoD telework policy, issued in response to the "Telework Enhancement Act of 2010,"[7] is for telework to be "[a]ctively promoted and implemented throughout the DoD in support of the DoD commitment to workforce efficiency, emergency preparedness, and quality of life…."[8] This policy extends the requirement for mobility computing from the tactical edge to the entire DoD enterprise. In doing so, it serves as an impetus for the implementation of a DoD enterprise architecture that makes data and services available to users anytime and anywhere, whether the users are at the office, at home, on the road, or on the battlefield.
- Outcomes of recent ICT Programs of Record. The track record of DoD Programs of Record, like Joint Tactical Radio System (JTRS), that have suffered from recurring cost and schedule overruns, and then, in the end, been overtaken by remarkable advances in commercial ICT, have caused the DoD to reconsider its acquisition strategies. The goal is to establish an agile acquisition process, designed to help the DoD overcome the innovation gap—the so-called *window of vulnerability* when the capabilities of adversary systems utilizing the latest commercial technology exceed those of the notional program of record system—illustrated in **Error! Reference source not found.**. In **Error! Reference source not found.**, the vulnerability gap is illustrated through the evolution of the cellular market[9], along with JTRS program development. The JTRS program started in 1997, was cancelled in 2012 after spending $6.7B, but recently fielded some radios[10],[11]. The JTRS radios do incorporate critical Transec capabilities and support tactical waveforms not available in the commercial cellular phones, although the transmission

[6] CHIPS, "Interview with Army Director CIO/G-6, Lt. Gen. Jeffrey A. Sorenson," CHIPS, October–December 2009, http://www.doncio.navy.mil/uploads/0109DJX21698.pdf.
[7] Public Law 111–292, "Telework Enhancement Act of 2010," December 9, 2010, http://www.gpo.gov/fdsys/pkg/PLAW-111publ292/pdf/PLAW-111publ292.pdf.
[8] DoD Instruction 1035.01, "Telework Policy," April 4, 2012, http://www.dtic.mil/whs/directives/corres/pdf/103501p.pdf.
[9] Kumar, Amit, Liu, Yunfei, Sengupta, Jyotsna, Divya, "Evolution of Mobile Wireless Communication Networks: 1G to 4G," InternatIonal Journal of Electronics & Communication Technology, Vol. 1, Issue 1, Dec., 2010, pp. 68-72.
[10] Rosenberg, Barry, "From radios to waveforms: How JTRS is remaking itself as JTNC," Defense Systems, Sep. 6, 2012, http://defensesystems.com/Articles/2012/09/06/Interview-Williamson.aspx?p=1
[11] Harris Corp., "Wideband Radio Makes Battlefi eld Networking a Reality," Tactical Comms Journal, Sept., 2009, http://rf.harris.com/media/FREQUENCY_WIDEBAND_RADIO_MAKES_BTFLD_NW_REALITY_tcm26-12152.pdf.

rates are significantly less. Rifleman radios using the Soldier radio wave form can transmit data from 200kbps to 1 mbps, while the Wideband Wave From is specified at up to 5 mbps.

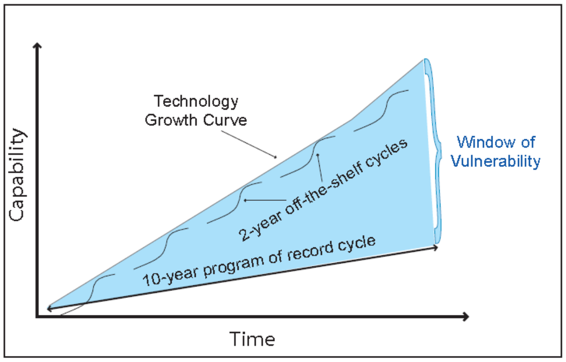


Figure 1. Off-the-Shelf Technology Versus a Program of Record Capability Cycle[12]

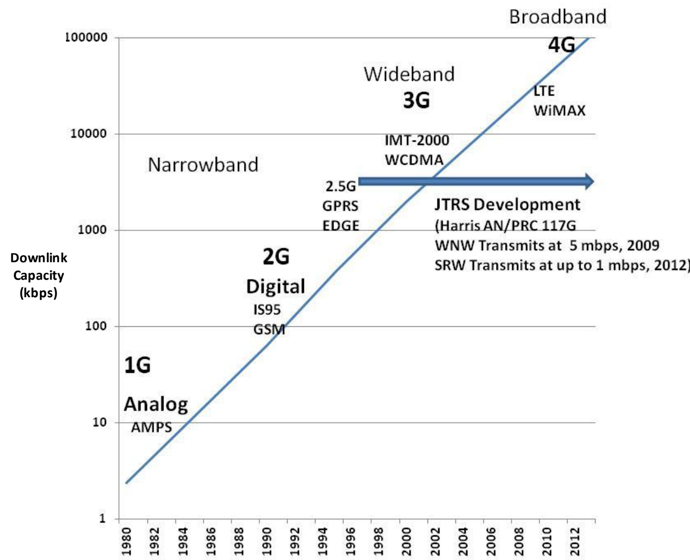


Figure 2. Evolution of Cellular Technology since 1980 and JTRS Program of Record Timespan

In pursuit of more agile acquisition, the Army is holding a series of biannual Network Integration Evaluation (NIE) events at which commercially-based ICT is tested by soldiers in the context of a Brigade Combat Team at Fort Bliss, TX.[13] The NIE requires vendors to demonstrate their equipment interoperating in a realistic environment with other existing equipment, prior to purchase. However, there is still a need for a process for acquiring those devices that show promise in a timely manner in order to keep industry motivated and participating.

3 Tactical Edge Challenges

Although the commercial devices supply great utility in the commercial environment, their use by the warfighter at the edge presents a variety of difficulties in realizing their promise. The conditions faced by the soldiers at the tactical edge are vastly different from the assumptions made for most commercial ICT products. This has led to a long history of the DoD developing its own solutions for communications and computing applications.

At the tactical edge, the network and computing infrastructure is deployed along with the rest of the soldiers and their equipment. There may be existing commercial infrastructure or there may be nothing.

---

[12] Source of Figure: K. J. Cogan and R. De Lucio, *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) During Operation Iraqi Freedom Combat Operations (Mar-Apr 2003), Volume II: Command, Control, Communications and Computer Architectures*, United States Army War College, 2003, Figure 33, p. 73, http://www.carlisle.army.mil/dime/documents/NCWCS%20Volume%20II%20%28web%20version%29.pdf.

[13] http://www.bctmod.army.mil/nie_focus/index.html.

The tactical edge networks must be portable and support mobility. This puts a heavy emphasis on wireless technologies and small, lightweight devices. Some of the unique requirements of the tactical edge for developing specific products and capabilities in the ICT domain are listed in Table 1[14].

Interoperability of new equipment and capabilities with the existing legacy equipment is a key requirement. The Global Information Grid (GIG) is the existing DoD communications infrastructure providing both enterprise and tactical communications and computing solutions. The GIG itself employs a mix of military specific and commercial technologies such as satellites, fiber optic communication equipment, routers, switch, security sensors and many others. Portions of the GIG are devoted to the warfighter at the tactical edge and include a range of solutions for the dismounted soldier, vehicles, ships, and planes. The introduction of commercial technology at the edge must integrate and be interoperable with the existing tactical portions of the GIG in order to be effectively utilized.

Table 1. Communication Technology and Environment Related Issues

Interoperability/Integration	With existing tactical network equipment – JTRS, WIN-T (JNN) and WIN-T INC 2
Disconnected, Intermittent, and Limited (DIL) Communications	Delay Tolerance
	Mobile Ad Hoc Networks (MANETs)
	Loss of infrastructure
Security	Cyber Attacks
	Encryption for data at rest/data in transit
	LPI/LPD
	Antijam
	Anti-spoof
	Authentication – 2 factor, biometrics
	Cross domain
	Patching
Environmental Factors	Rugged, water proof
	User interface -sun glare, night vision mode, low light, touchable with glove
Acquisition	Supply-chain considerations
Network Operations and Management	Spectrum
	Remote auditing
	AAA – logging
	Monitoring
	Loss of infrastructure
	Capture of equipment (remote wipe)
	Remote peripheral control
Size, Weight, and Power (SWAP) Constraints	Power requirements, battery life, battery type
	Portable
App Management	App ecosystem

[14] Office of the Department of Defense Chief Information Officer, *Department of Defense Mobile Device Strategy, Version 2*, May, 2012, http://www.defense.gov/news/dodmobilitystrategy.pdf.

Another key requirement is the need to be able to continue operations in the face of hostile actions that cause loss of major portions of the infrastructure, often deliberately targeted to cause maximum disruptions. Commercial systems must be robust in the face of equipment and link failures, although acceptable recovery time may be longer in the commercial world. Methods to continue operations in the face of intermittent connectivity, such as Delay Tolerant Networking protocols, are still under development by the government, but with limited demand from the market. Research into robust Mobile Ad Hoc Networks (MANETs) has long been sponsored by the DoD. So far, these are being implemented in several military systems, but have found limited adoption in the commercial environment. This may change as car-area networks begin to emerge, driven by the auto industry.

Security is frequently cited as the major factor that limits the utilization of COTS. Again, the consequences of breaches or other security failures are much higher in the warfighter domain than most others. There has been a great deal of development of tactical radio technologies to provide transmission security through methods to insure Low probability of intercept /Low probability of detect (LPI/LPD), anti-spoofing and anti-jam capabilities. Anti-spoofing and LPI can be somewhat mitigated by encryption technologies, but the commercial environment does not really address LPD, other than by the general trend of lowering transmission power and increasingly sensitive receiver technology. It is well known that it is fairly straight-forward to jam commercial access points or base stations. Also, it is relatively simple to direction-find the source for most commercial signals (such as wi-fi or cellular). Military techniques such as frequency hopping, spread spectrum or ultra-wide band have not garnered wide commercial adoption.

The DoD also has a relatively unique need for multiple levels of classification and requires better means to share networking infrastructure and to permit cross-domain solutions. This does not appear to be addressed in the commercial market.

Encryption has been a DoD-unique requirement, with hardware and software methods strictly controlled by the National Security Agency (NSA), addressing protecting data-at-rest and data-in-transmission. In the security arena, the DoD requirements are viewed as being more stringent than that required in the commercial world. There was an attitude in the DoD that all communications must be highly secure, requiring specialized hardware encryption. However, recently, there is recognition that not all communications require this level of protection and that many of the commercially available, software-based encryption can be used. For example, some temporal information can be encrypted with common methods, such as AES, since by the time an adversary decrypted the message, it would have little value.

Another aspect of security is the vulnerability to cyber-attack. Hacking attempts on military and commercial systems are increasing at a steep rate and identify theft is rampant. Both sectors are investigating solutions. COTS equipment, such as Android-based smart phones attract a large number of potential hackers, due to its large market share. Military systems, on the other hand, represent high value to a relatively small number, but highly capable cyber-attackers. A related issue involves patching and upgrading of equipment software. If COTS devices are employed then the patches are supplied by vendors and must be managed and distributed through their tactical network. This requires testing and

vetting of the patches prior to distribution. In some cases, there are multiple providers of patches that must be managed, such as with Android OS on smartphones or tables where they can come from the developer (Google), the device manufacturer (e.g., Samsung, HTC) and the cellular provider (e.g., AT&T, Verizon). Further, if there has been customization of the devices, then the patches or upgrades may cause problems with the customization, which the DoD vendor must quickly address, requiring long term relationships with those vendors.

Authentication is a difficult issue for both military and commercial systems. For the tactical edge, simple and effective methods that can be used under conditions of extreme stress are needed. Biometric techniques and hardware tokens are more appropriate than complex passwords. In the commercial world, as consumers do more financial and personal transactions, authentication is also improving, but cumbersome methods are still being utilized.

The requirements for ruggedness are clear. Other factors such as the need for displays operating with night vision equipment, protection from others with night vision equipment are unique. Similarly, size, weight and power (SWAP) are critical to soldiers already burdened with large amounts of equipment. The trends to reduce SWAP coincide with the trends in the commercial market and advances should continue from their development activities.

The DoD desires tight control and situation awareness of the networks, much as the commercial providers maintain, but the highly mobile, stealthy and dynamic nature of the tactical networks makes this a challenge and a large collection of DoD specific tools has resulted. The ability to obtain battle damage assessments and to rapidly reconfigure the network is crucial. Currently, there is a large amount of commercial development activity on network operations and management, in particular concerning cyber-defense where there is a need to gain a better understanding of the realtime status and of the network in order to defend and recover from both physical and cyber-attacks. The capability to obtain forensic information to diagnose and correct problems through extensive AAA is needed in both domains.

The need to be able to remotely wipe a device that has fallen into the wrong hands is critical for the tactical edge where devices may be able to reveal the locations of other blue forces. In addition, it may be desirable to remotely control the peripherals on a device for sensing or other administrative functions. Commercial vendors are also working on these issues and may be able to provide solutions in the near term.

Another differentiating factor for the military, related to security, is the supply-chain consideration. Most of the electronics in the equipment and more and more of the software are supplied by foreign vendors. This presents a risk that the devices may be tampered with or otherwise modified to compromise the equipment. The DoD sometime resorts to manufacturing the equipment under its control, but this is an expensive process. It may be possible to reduce this risk by purchasing commercial commodity products where it is not known that they will be used by the DoD.

In the area of Apps for smartphones and tablets, there is need to improve the entire management of the App life-cycle: Development/Attestation/Acquisition/Distribution. There will be need for some

development of specialized apps for use at the edge, but there seems to be many more opportunities for limited customization of existing commercial apps. It is likely not possible to build a thriving app community of only DoD users because there is not a sufficient critical mass of users to drive the innovation. It would seem more prudent to take a MOTS approach.

Many of the DoD requirements have clear dual-use applicability, but often the consequences of an imperfect solution are much greater for the military. In this case, both fundamental and applied R&D and customization are likely to be needed.

4 Current and Near-Term Application of Commercial ICT at the Tactical Edge

The DoD is embracing commercial technology and all its associated benefits, despite the challenges discussed above. In this section, we discuss three kinds of technology: 1) end user devices, such as smartphones and tablets, 2) apps and an app store associated with the end user devices, and 3) the communication infrastructure that enables their use.

4.1 Smartphones and Tablets

Commercial end user device technology is already being applied to the tactical environment. In some cases, commercial smart phones are being used as is; however, in other cases they are being adapted to the special needs of the tactical environment. Vendors are undertaking some of the adaptations, because they see a growing market for secure, ruggedized devices that can be used not only in the military domain, but also in public safety, disaster relief, humanitarian aid, and wilderness domains. Other adaptations are being pursued by the DoD and the Intelligence Community. In these cases, the essential properties of the devices are being preserved; for example, the ability to run third-party apps is retained by employment of the Android operating system. Commercial chipsets, such as LTE chipsets, are also being used.

Commercial Mobile Device Technology Targeted at Military and Related Markets

Vendors, including both defense contractors and others, are providing more secure, ruggedized versions of smartphones and tablets, retaining their key features but adding others, as illustrated in Figure 3. One of the devices in the figure is a **Harris RF-3590 ruggedized tablet**,[15] whose features include internal GPS, gyroscope, and digital compass; front and rear (8-megapixel) facing cameras; noise canceling microphones; internal Bluetooth transmitter (for optional wireless speaker microphone); WiFi capable; broadband video, voice, location, and text-based communication; SD and USB ports; interchangeable high-capacity battery, and Android tablet OS.

Another approach to adapting commercial devices to specialized environments, such as public safety, is taken by BriCom Solutions, LLC, which provides a portable docking device (**Alianza Docking Cross Breed (DxB)**) that enables a commercial smartphone to operate as a fully-functional two way radio. Together,

[15] http://pspc.harris.com/LTE/BTC100.asp

the smartphone and the docking provide public safety personnel traditional two-way radio communication capability as well as access to Internet, video, camera and applications.[16]

Figure 3. Convergence of Commercial, Military, and Public Safety End User Devices

Smartphone as Complement to Tactical Radio: Nett Warrior

Nett Warrior is a fast track program to bring command and control network capabilities to the foot soldiers on the ground.[17] It is a basic, ruggedized smartphone that is mounted to a soldier's wrist, chest or arm. The device plugs into the existing AN/PRC-154 Rifleman Radio, one of the JTRS radios already fielded in order to communicate over the tactical network. The proposed system includes the ability to project battlefield maps and unit location data to the user. Currently, a new acquisition process is being tried so that multiple vendors can offer competing smartphones that will be tested at a Network Integration Evaluation exercise in May, 2012. The concept is not to deliver these to every soldier, but to leaders of 4-man teams at this time. One early advantage of the Nett Warrior program is that the newer smartphone device replaces the original concept of having a backpack computer with a small display that flipped down over one eye and weighed around 14 pounds.[18] The ability of the device to integrate with the JTRS radio should greatly increase its viability. However, early reports from the field tests indicate that it is not yet ready for actual use, primarily due to issues with the capability to locate neighboring friendly soldiers that also have Nett Warrior [ref?].

---

[16] http://www.bricomsolutions.net/Product/RoIPProducts/Hardware/Alianza/index.html

[17] Liam Stoker, "Battlefield smartphones receive a ringing endorsement," ArmyTechnology.com, 31 July 2012, http://www.army-technology.com/features/featurebattlefield-smartphones-endorsement-technology

[18] Freedburg, Sydney, "Army Seeks New Network Tech for New Brigades Post Afghanistan," AOL Defense, Mar. 19, 2012, http://defense.aol.com/2012/03/19/army-seeks-new-network-tech-for-new-brigades-post-afghanistan-m.

Ongoing DoD and IC Efforts to Enhance Trust and Security: USMC Trusted Handheld Platform and NSA Fishbowl

The **US Marine Corp** has recently initiated the **Trusted Handheld Platform** program aimed at adapting commercial mobile device technology for secure communications. The goal of the project is to field commercial smart phones with standard hardware and software that are capable of accessing the military's classified and unclassified networks. The phones will be able to send and receive secure voice, data and video across security domains. Several key commercially-based technologies will be incorporated in the devices including virtualization and isolation methods including domain separation, process isolation, and resource encapsulation. Additional features that are desired include hardware root of trust, trusted boot, and Suite B encryption meeting FIPS 140-2 certification from NSA. The solutions must be designed in a modular fashion to avoid reengineering of the commercial devices. The project involves a collaboration with government and industry to speed up the certification process and also to result in device capabilities that can be adopted into future commercial versions. "The military and the commercial market share a common need – a highly-secure, low-cost mobile device solution to share and manage sensitive content across their networks," said Thomas Harvey, Senior Vice President, AT&T Government Solutions. AT&T, one of several contractors, will provide 450 prototype device based on the Android OS, but eventually the trusted platforms should support other devices and operating systems[19],[20],[21].

The **NSA pilot project Fishbowl** is effort to provide secure communications over commercial cellular network using commercially available Android-based smartphones. Their approach was to provide a voice service using Voice Over IP encrypted with a second layer of software encryption in addition to the encryption provided by the vendor.[22] In the future, they will expand to also provide data capabilities. The phones will allow two users with the Fishbowl devices to have a secure classified conversation over the commercial cellular network. Currently, the pilot is evaluating the performance and security of the devices using over 100 fielded phones. The experiences have provided important inputs to the development of a "Mobility Capabilities Package" with industry security guidelines.[23] Some issues that the project is still working on include what to do about over the air updates and how to transition from inside a secure SCIF to an unsecure network. The long-term goal is to provide these capabilities to the warfighter.

---

[19] Kenyon, Henry, "Marines want smart phone for classified, commercial systems," GCN, April 2, 2012, http://gcn.com/Articles/2012/04/02/Marine-Corps-launches-trusted-mobile-device-program.aspx?Page=1

[20] US Marine Corp, *Pre-Solicitation for Trusted Handheld Platform*, M6785412I2414, Nov. 11, 2011, https://www.fbo.gov/index?s=opportunity&mode=form&id=122a0b90a671494db0e365f018ac7d12&tab=core&_cview=1

[21] AT&T, "AT&T to Develop Highly-Secure, Commercially-Available Mobile Devices for Military and Enterprise," PR Newswire Oakton, VA 12-19-2012, http://www.bloomberg.com/article/2012-12-19/aIAC_fSKajZ0.html

[22] Iannota, Ben, "Top Secret Goes Mobile," Defense News , Mar. 29, 2012, http://www.defensenews.com/article/20120329/C4ISR02/303290008/Cover-Story-Top-Secret-Goes-Mobile.

[23] National Security Agency (NSA), *Mobility Capabilities Package: Secure VOIP, Version 1.1*, Feb. 27, 2012, http://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_(Version_1.1U).pdf.

Ongoing DoD Effort to Enhance Robustness: MACE

One effort that is looking into inserting commercial smartphone technology to improve C3 is the **Multi-Access Cellular Extension (MACE)** program.[24] The benefits of smartphone technology is that it supports bundling of functions, such as voice, data, military-purposed smartphone applications, and position/location information into a single device to save weight, space, and power. MACE employs radio frequency ranging to determine location in GPS-challenged environments. The MACE program uses a mixed WiFi cellular base station connected to a tactical network such as the Warfighter Information Network–Tactical (WIN-T). WiFi mesh networking allows groups of soldiers to form LANS and communicate when the base station is not available.

4.2 Apps and App Store

Part of the popularity of smartphones has been the volume and range of applications that are available as well as the relatively low cost and straight forward means of downloading them from the Application Store. In October 2012, Android applications were reported to be as much as 700,000, equaling the number reported for Apple's IOS.[25] In particular, various vendors have built application infrastructures around the various mobile phone operating systems (OSs) such as Android and IOS, that are now supporting both smartphones and tablets. The Android OS is very popular with developers due to its open source code and interfaces that supports customization of the software that more closely interacts with the hardware than is possible with other OSs.

Table 2: Commercial App analogs to military capabilities

Military Capability	Similar Commercial Smartphone/Tablet Apps
Command and Control	Chat/IM, SMS, MMS, voice call, video call, Twitter, email, Skype
Mission Planning and Execution	Electronic Flight Bag
Situation Awareness (Blue Force Tracking)	WAZE, Google Maps/Earth, StarChart, Location-based Apps, News feeds
Streaming Video	YouTube, Hulu, Crackle
ISR	Home Monitoring, Friends Tracking, Picture tagging
Soldier as a Sensor	WAZE, Ratings
Biometrics	Face, Voice, Keystroke, IRIS Recognition, fingerprint matching, browsers
Secure, Hands-Free Communications	WICKR, Speech-to-text, Siri
Information Sharing, Access	Dropbox, browsers, Splashtop Whiteboard
Document and Media Exploitation (DOMEX)	Google Translate, iTranslate, Mobile OCR
Education, Training	YouTube, Wikipedia, Dictionary,
Personal applications	Alerts, financial, social media, shopping, games, etc

[24] Edwards, John, "Tactical radios and mobile devices: Powered by imagination," Defense Systems, Apr 03, 2012, http://defensesystems.com/articles/2012/03/28/cover-story-tactical-radios-mobile-devices.aspx

[25] Tibken, Shara, "Google ties Apple with 700000 Android Apps," CNET, Oct. 30, 2012, http://news.cnet.com/8301-1035_3-57542502-94/google-ties-apple-with-700000-android-apps

In Table 2 some sample commercial applications that could provide useful functionality for warfighters or could serve as a template for customized functions are listed. For example, WAZE is a navigation app where users post information on traffic, speed cameras, and other useful information to a common map display. Another example, WICKR provides encryption for secure conversations among friends. Electronic Flight Bag is an Air Force application that is used to replace pilot's paper maps on an iPad tablet computer.

Given a communications capability there is also an expectation of applications that can utilize the computing power of these devices, typically by pre-installing or downloading applications. Downloadable apps are usually managed by a provider through an apps store which vettes (provides a quality and validation check as well as authentication). Even if pre-installed, apps will usually require connectivity to a data server for updating periodically to obtain security or functional upgrades.

The DoD has selected the Army App Store or US Army Mobile Marketplace as its method of distributing approved applications.[26] As of Feb. 2013, the app store had about 25 applications with the last contribution in July.

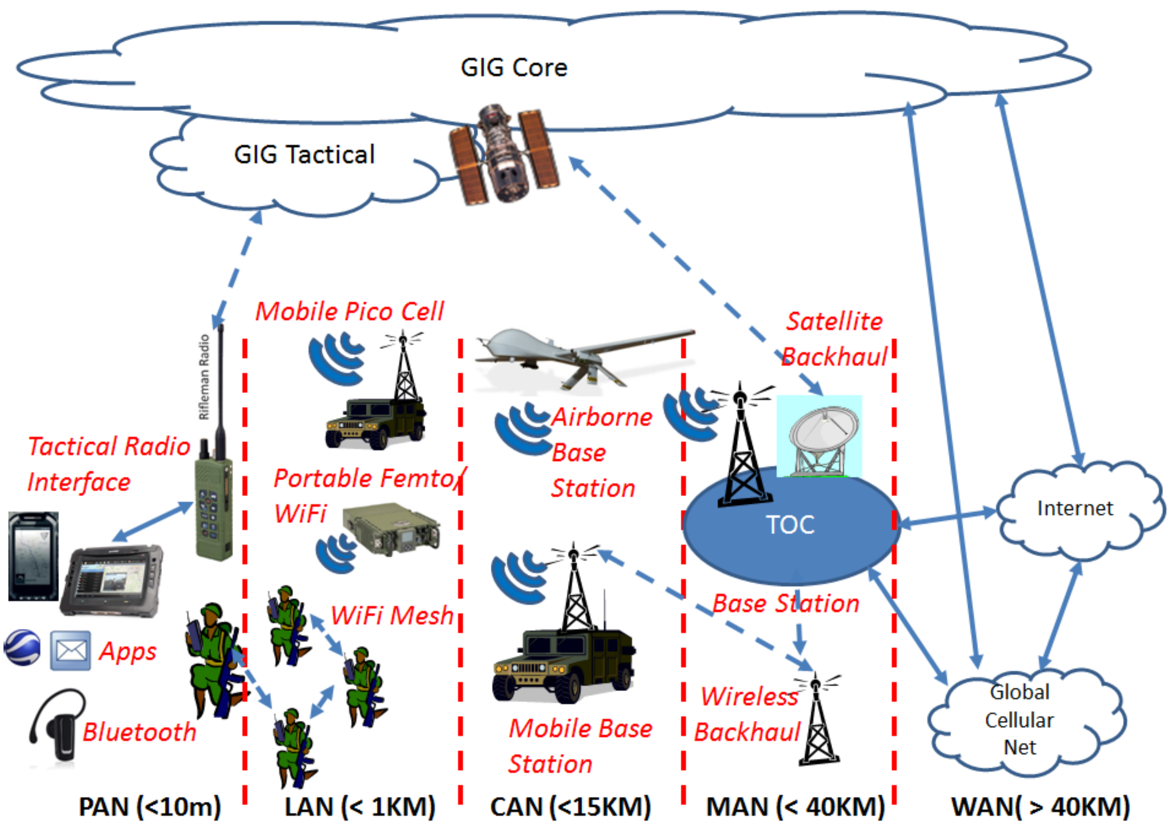


Figure 4. Application of Commercial Technology in the Tactical Networks

---

26 www.army.mil/mobile/

4.3 Tactical Edge Communication Infrastructure

Commercial solutions to enhance the tactical edge communication infrastructure are being applied and investigated by the services. In Figure 4, some examples of commercial technologies that are being considered for tactical network application are shown. Commercial networking technology is often considered in terms of distance of communications such as Personal Area Networks (PANs) or Body area networks (BANs) for under 10m, Local area networks (LANs) for up to 100m, Campus area networks (CANs) (100m to 10 km) including backhaul, Metro Area Networks (MANs) and Wide area networks (WANs) for greater distances. The DoD has requirments across all these distances and due to mobility requirements and lack of infrastructure in remote areas, wireless solutions are often the only viable solution.

Technology appropriate for PANs includes Bluetooth to connect with ear-piece-microphones. Other examples include wearable components such as a Personal Digital Assistant (PDA) worn on an arm, or a head-mounted display or sleeves that can interface to tactical radios. Technology appropriate for LANs includes a wide variety of choices such as WiFi and various cellular adaptations such as femto and pico cells. Many smart phones and handhelds support both WiFi and often several types of commercial cellular connections. The advantages of WiFi include higher data rates and widespread use and ease of setup as well as ad hoc or mesh networking. Long haul networking can use either the existing GIG, Commercial Cellular, Global Fiber network or commercial satellites providing options for reachback communication paths. The GiG already employs both military satellites and frequently leases capabilities from commercial suppliers.

Table 3 offers an overview of all the regimes from PAN to WAN. Below, we focus mainly on the LAN to MAN regimes and describe two classes of solutions: 1) cellular infrastructure, including small cellular base stations, and 2) alternatives to the tactical radios envisioned, and in a few cases, delivered by the JTRS Program of Record.

4.3.1 Cellular Infrastructure

The ability to rapidly deploy cellular infrastructure has been pioneered for the first-responder community in response to natural or other disasters such Katrina or 9/11 attack. After Katrina, a 3G Pico cell base station was deployed on a rooftop in downtown New Orleans. The local carrier allowed the use of its frequency spectrum since its service was completely knocked out by the hurricane. Pre-registered handsets were distributed to key officials, Local calls to others within the private network were accommodated and a satellite terminal was employed as a gateway to the working cellular phone network in California.[27]

[27] Varga, Robert, "COMM-OPS: UAV Cellular Payload for First Responder Emergency Teams," MILSAT Magazine. July, 2009, http://www.milsatmagazine.com/cgi-bin/display_article.cgi?number=1435005486

Table 3. Commercial Technology and Military Analogs

Communication Regime	Commercial Technology	Commercial Examples	Application	User Mobility	Infrastructure Mobility	Military analog/Example/Prototype Adoption
PAN	Bluetooth, NFC	Embedded in smartphone, table	Ear-Mic, Headmounts, Authentication	Dismounted		Wired, tethered interfaces CAC smartcard
	GPS	Embedded in smartphone	Location-based applications			PLGR, DAGR
	USB, Sleeves		Interface to Tactical Nets			Intf to Riflemanr Radio, SINCGARs MONAX
LAN	WiFi APs, MiFi Hotspots, Femto cellular	AT&T Femto cell	Voice, data, video	Dismounted	Fixed or Portable	Knightlite, JTRS Rifleman Radio, SINCGARS
	WiFi Mesh		Voice, data,	Dismounted	Portable	MACE App(Mesh), JTRS Rifleman Radio MANET, Harris 117G
CAN	3G, 4G LTE Mobile Base Station	ATT ARMZ, LGS Pico, Qualcomm, Vanu,	Voice, data, video, position	Mobile	Portable	KnightHawk, LM MONAX, SRW Appliqué, MNVR
	Airborne Base Station	AirGSM	Voice, data, video	Mobile	Portable	FASTCOM, BACN, LM MONAX
	Backhaul	WiBack, Many Satcom providers	Backhaul for control and data		Fixed, Portable	WIN-T
MAN	3G, 4G-LTE Base Station	Many commercial providers	Voice, data, video, position	Mobile	Fixed or Slowly mobile	Navy WWAN

A typical cellular base station provides some of the functions necessary to provide a connection service and relies on the existing cellular infrastructure to provide the others through the backhaul link. The major functions of a cellular system (loosely adapted from the GSM standard) besides the Base Transceiver Station (BTS) that contains the radio include a base station controller for resource allocation, user registration service, and support for connecting to phone, cellular and internet networks. In 4G systems, all traffic is IP so that some of the above functions can be combined. In military applications, a survivable base station should be self-sufficient, containing all of the hardware and software needed to configure and manage the network services without reliance on the backhaul service. This allows local communications between users in the coverage area to continue if the backhaul connection is lost (not typically required on commercial offerings).

Microcells such as Pico cells and Femto cells are essentially simplified macro cellular base stations operating at less power and provide a localized cellular service. They require a backhaul connection to a cellular server, for example, through the internet, to obtain some of the functions normally provided by a cellular base station infrastructure. A Femto cell typically handles 10s of users up to a range of 100m while a Pico cell handles 10-20 users over a 500m-1000m range. The advantage of these devices is their compatibility with commercial cellular systems and relatively easy setup. The backhaul demands of Femto and Pico do not require as high a capacity as a full cellular base station, although performance of the cells depends on the response times to/from the backend server to provide the missing cellular services. These are small, lightweight, and portable and are often be configurable to handle local communication between users in the same cell without the backhaul link. Often, they are able to also supply a WiFi hotspot capability. For vehicle communications, pico or macro cellular technologies can provide a solution for communication at vehicular speeds. These gemerally require a higher-power base station along with appropriate antenna and power generation capabilities and are typically mountable on a vehicle.

In large, fixed base applications supporting the warfighters, standard (hardened) commercial base stations can be employed effectively to support dismounted and mounted users. The backhaul can be accomplished with wired or wireless connections to either the commercial infrastructure or the GIG. Wired can be copper or fiber connections but wireless would typically be satellite based, although wireless mesh backhaul schemes have been put forward.

For mobile command posts or temporary deployments, hardened mobile base stations that can be quickly deployed and that can be used on a variety of platforms such as armored vehicles are required. These mobile command posts will typically use a backhaul connection for reachback to the GIG and would typically be served by a satellite communications terminal co-located on the vehicle. The base stations are designed with enough computation power to handle the additional cellular functions and will often also handle gateway or bridging functions between various commercial and military networks.

Commercial Products Targeted at the General Market

AT&T has developed a cellular base station that can be deployed for civilian applications in remote locations called the **AT&T Remote Mobility Zone (ARMZ)** system.[28] It provides a GSM Picocell base station which can be connected to a satellite link used for the backhaul to the AT&T Cellular core network. It can also interface to the internet through other types of backhaul solutions. Each picocell runs 2.5G EDGE protocol for voice and data and can support 2 radios each carrying 14 simultaneous users and requiring a backhaul capacity of 384 kbps. The system can be deployed in a fixed or mobile mode and is easily set up. It can only operate in the US where AT&T owns the spectrum.

Commercially-Based Technology Targetted at Tactical Edge

The **KnightHawk** system by Harris provides commercial cellular capability in a small box that supports fixed locations operation or can be vehicle mounted. It supports 3G Universal Mobile Telecommunications Technology (UMTS) and High-speed Packet Access (HSPA) networking protocols.[29] The system supports standard smartphones equipped with special SIM cards. The base station can operate autonomously or as part of a larger network where multiple KnightHawks can be linked together, increasing range and user and data capacity. KnightHawk is self-contained WCDMA cellular network operating in the 2100-MHz band. This single carrier high capacity wireless base station provides 10 watts of power output, features a capacity of up to 20 simultaneous voice calls and 14 HSPA data connections extendable to 60 simultaneous voice users. It weighs 36 pounds. The devices contain configuration and management software. There is also a man-portable version called **KnightLite** which can be mounted in a vehicle or carried in a backpack. The manpack includes the battery and can be interfaced to a tactical wireless link for backhaul purposes.

In 2012 the Navy began deploying a 4G LTE-based **Wireless Wide Area Network (WWAN)** on several of its ships. The system, under development since 2009 and now undergoing final testing, is a ruggedized LTE network, similar to commercially provided versions, that can operate in a mobile, ocean environment. The Navy WWAN will work at distances up to 20 nautical miles and provides aggregate throughput of up to 300 mbps. The system will allow sailors and marines to communicate voice video and data with other users, nearby patrol boats, ships, drones, planes and helicopters within the coverage area using Android-based cell phones. WWAN provides much need communication capacity that was previously only provided through the capacity-limited satellite connections (additionally freeing up those connections from local needs). For example, they can receive video feeds from the helicopters that could be used for better situation awareness in anti-piracy operations. Currently, the Navy WWAN is not connected to the satellite tactical networks.[30],[31]

[28] AT&T, "AT& T Remote Mobility Zone (ARMZ) System," https://www.wireless.att.com/businesscenter/en_US/pdf/att-remote-mobility-zone-product-brief-062712.pdf

[29] Harris Corp., "KnightHawk," http://www.govcomm.harris.com/solutions/products/isr/knighthawk.asp

[30] Ackerman, Spencer, "In First, Navy Will Put 4G Network on Ships," May 23, 2012, Wired Magazine, http://www.wired.com/dangerroom/2012/05/navy-wwan/

[31] Ackerman, Spencer, "Navy's First 4G Network Will Head Out to Sea in March," Wired Magazine, Feb. 6, 2013, http://www.wired.com/dangerroom/2013/02/navy-wwan-deploys/

The aerospace industry has been moving forward with incorporating Pico and Femto base station technologies on commercial aircraft to provide flyers with the ability to use their cell phones. Typically, a satellite link is employed for the backhaul. There have been various approaches to host cellular base station technology onto a plane, UAVs or lighter-than-air platforms to provide ground cellular coverage over a larger area than possible with towers or building rooftops. With advancements in UAV technologies coupled with miniaturization of base station components and better batteries, UAVs seem an attractive alternative. UAVs have increasing abilities to hover over an area to provide the coverage (the predator can remain airborne for over 24 hours). One example is a **small GSM-based fully functional cellular base-station has been shown to fit into a small hovering UAV platform and connectivity to commercial handsets** has been demonstrated; however, only limited feasibility testing has been reported to date.[32] Another system developed for military applications is the **Forward Airborne Secure Transmission and Communication (FASTCOM)**, a mobile, secure battlefield cellular network that can be placed on a UAV.[33] FASTCOM uses a Pico cell base station on pods mounted on the drone, communicating with users with smartphones on the ground and a ground-based data terminal for backhaul into the tactical network.

The Air Force has successfully deployed an airborne gateway system, called the **Battlefield Airborne Communication Node (BACN)**, that extends communications ranges and bridges between various tactical and civil cellular links including UHF/VHF, first responder radios and commercial cellular systems.[34] However, performance data on the cellular capabilities is not available. BACN is flying on several E-11A Global Express long-range business jets and EQ-4B Global Hawk Block 20 UAV variants.

4.3.2 Tactical Radios: Alternatives to Program of Record Devices

The failures of the JTRS Program of Record have motivated the DoD to turn from long-term, large-scale, government-ruled development efforts to more agile acquisition schemes, prompted by internal development activities of the vendors. Below, we offer brief descriptions of the various steps the DoD is taking in this regard.

Mid-Tier Vehicular Radio (MNVR): Agile Acquisition to Replace a Failed Program of Record

The JTRS Ground Mobile Radio (GMR) Program was launched in 2002 to develop a multi-band, multi-mode, software-defined, vehicle-mounted radio hosting seven waveforms—including Wideband Networking Waveform (WNW), Soldier Radio Waveform (SRW), and the legacy SINGCARS waveform—and intended to provide communications across the tactical domain. After a decade and billions of dollars, when the radio was still not meeting its requirements, the DoD terminated the JTRS GMR Program. However, the DoD did not abandon the entire concept of the GMR. Instead, the DoD decided to acquire an alternative—a small, affordable, focused variant having only two rather than seven

---

32 Wypych, Tom, Angelo, Radley, Kuester, Falco, "AirGSM: An Unmanned, Flying GSM Cellular Base Station for Flexible Field Communications," IEEE Aerospace Conference, March, 2012, pp. 1-9.

33 AAI Corp., "FASTCOM Mobile Communications Network," 2010, http://www.aaicorp.com/pdfs/AAI_FASTCOM%2010-18-10FINAL.pdf

34 Defense Industry Daily Staff, "Bringing Home the BACN to Front Line Forces," Defense Industry Daily, Nov. 4, 2012, http://www.defenseindustrydaily.com/bringing-home-the-bacn-to-front-line-forces-05618/

waveforms. As stated by the Undersecretary of Defense for Acquisition, Technology and Logistics in his letter to Congress terminating the GMR Program:[35]

> *As a result of the Department's investment in the development of software defined radios, software communications architecture and openly shared waveforms, a competitive market emerged with the potential to deliver radios to meet the capability at a reduced cost… [It] was determined that an NDI [Non-Developmental Item] acquisition approach was the most viable means to meet this requirement.*

The MNVR contract could be worth as much as $140 million. Vendors expected to offer solutions include General Dynamics, Harris, Raytheon, BAE Systems, and a Northrop Grumman/ITT Exelis team. Notably, the Harris JTRS-Certified Falcon III PRC-117G radio already serves the MNVR role in the Army's Capability Set 13, which has been defined over the course of a few NIE events for deployment to selected Brigade Combat Teams. Additionally, the Raytheon Maingate radio is already deployed in Afghanistan.[36,37]

JTRS Rifleman Radio: Fair and Open Competition for Full-Rate Production of a Program of Record Capability

The Rifleman Radio, the element of the JTRS Handheld, Manpack, Small Form Fit (HMS) family intended for use by soldiers at the platoon level and below, was developed via a program of record with General Dynamics and Thales Communication. It uses the SRW waveform and provides voice, data, and position services. The Army has committed to purchase close to 20,000 Rifleman Radios through low-rate production orders from General Dynamics and Thales. However, in the interest of leveraging commercially available technology to the extent feasible, the Army has decided to employ a fair and open competition for full-rate production of up to 80,000 or more radios.[38]

SRW Appliqué: Agile Acquisition of a Newly Defined Requirement

The Army is using an agile bidding process to acquire a capability—referred to SRW Appliqué because it adds a Soldier Radio Waveform (SRW) networking capability to vehicles via existing SINGCARS radio installations—that will a support communication between JTRS Rifleman Radios and the broader tactical network. General Dynamics C4 Systems, Harris, ITT Exelis, and Thales are viewed as likely bidders. Interestingly, the General Dynamics bid is based on their Rifleman Radio, and the Harris bid is based on their Falcon III AN/PRC-152A handheld radio, referred as Side Falcon.[39]

---

[35] Frank Kendall, Acting Under Secretary of Defense for Acquisition, Technology and Logistics, "Letter to the Chairman of the Senate Armed Services," 13 October 2011.

[36] D. Ward, "Tactical Radios: Military Procurement Gone Awry," National Defense Magazine, July 2012, http://www.nationaldefensemagazine.org/archive/2012/July/Pages/TacticalRadiosMilitaryProcurementGoneAwry.aspx.

[37] Excellis Inc., "Northrop Grumman, ITT Exelis Team to Compete for Army's Vehicular Radio," Press Release, 19 December 2011, http://www.exelisinc.com/news/pressreleases/Pages/Northrop-Grumman,-ITT-Exelis-Team-to-Compete-for-Army%E2%80%99s-Vehicular-Radio-.aspx.

[38] W. Welsh, "Army to open Rifleman Radio procurement to full and open competition," 22 October 2012, Defense Systems, http://defensesystems.com/articles/2012/10/22/army-solicitation-full-rate-production-rifleman-radios.aspx.

[39] J. Edwards, "SRW Appliqué and Agile Bidding: Vehicle Voice and Data," *Defense Systems*, 15 January 2013, http://defensesystems.com/Articles/2013/01/15/special-report-soldier-radio-waveform.aspx?p=1.

5 Future of Commercial ICT at the Tactical Edge

It is clear that military adoption of commercial technologies will continue, however, at a pace largely dependent on the ability to procure in a timely fashion.   It seems clear that when the military requirements coincide with the enterprise or consumer market requirements, then the commercial products can be easily adopted. There are two aspects of future developments that should be considered. These are 1) what technologies are emerging from the commercial R&D activities that can be applied to the military's needs, and 2) what gaps in the military's requirements are not likely to be addressed by current, emerging research and development.

In the later case, the DoD may need to invest in basic or applied R&D in order to try to develop technologies to fill these gaps. An example of an area that requires more research but does not have a great commercial application would be airborne networking. However, it is apparent from the earlier comments, that the results of research investment in these types of areas will need to be adopted with an understanding of the new environment.   The DoD has been successful in the past in funding seed research that has resulted in commercially successful and revolutionary technologies, such as the Internet.   However, the real success and advancement s for these technologies resulted from commercial development and the creation of the mass consumer market, rather than DoD applications.

In addition, as seen by the many examples cited earlier, the customization of commercial off the shelf products with limited modification, seems to be the way forward in many situations.   A desirable property is to engineer the modifications in a modular fashion so that the resulting product is still able to evolve with the underlying base commercial product. We call this Modular-off-the-shelf (MOTS) systems.   Given the rapid product cycles, the most cost-effective way to develop this property is not known. With this in mind, DoD S&T investments should focus both on early, basic R&D as well as applied R&D looking at methodologies for developing MOTS and managing the MOTS lifecycle.

5.1 Promising ICT R&D

Some examples of emerging S&T that are likely to impact the tactical networks are presented. As mentioned earlier, standardization is a key to reducing risk in commercial adoption. There are several interesting future network design concepts that are being discussed on the networking standardization stage: including Software defined Networking (SDN), Autonomic Networking, and Cognitive Radios for Spectrum Sharing.

Software defined networking defines an abstract virtual network that can be tailored to particular applications. The concept utilizes and open language, such as OpenFlow , and open interfaces that reside on commodity hardware that would be relatively inexpensive as compared to current network routing and switching equipment. SDN is being pursued in standards bodies such as the Open Networking Foundation (ONF)[40] and the Internet Engineering Task Force (IETF).[41] There are many

---

[40] Open Networking Foundation , "Software Defined Networking ," https://www.opennetworking.org/.

[41] Pan, P., "Software Defined Network (SDN) Problem Statement and Use Cases for Data Center Applications," IETF, 2011, http://tools.ietf.org/id/draft-pan-sdn-dc-problem-statement-and-use-cases-02.html.

potential DoD uses for SDNs in tactical networks, such as creating rapidly reconfigurable networks, implementing coalition networks, creating high-security enclaves , or instantiating security-aware networks , all using commodity network routing equipment. Academic research is continuing in this area at a rapid pace. Commercial vendors are now beginning to offer products that provide varying degrees of SDN capabilities for special applications such as data centers and this should be an increasingly important capability in the near future.

The Autonomic Networking activities are looking at several concepts such as self-organizing networks (SONs) and autonomous architectures. SON concepts, such as plug and play for Femto or Pico cells address the ability of the small base station to allocate the radio and network resources such as channels and rates to its users in a distributed fashion, rather than centrally controlled. The 3GPP/SA5 standards group is considering self-configuration, self-healing and self-optimization. Preliminary results for SON for LTE have been released.[42] Standards are being addressed in the ITU and 3GPP forums. A related activity in the ETSI Enhancing ETSI Network Activities project is examining Autonomic Network Engineering for the self-managing Future Internet. They are coming up with "autonomic-aware" architectures to incorporate a degree of intelligent behavior in the self-managing Future Internet.[43] These capabilities have clear potential to improve the survivability and ease of set up of tactical networks.

Cognitive radio or spectrum sharing research has been primarily driven by government investment such as through NSF and the DoD. Cognitive Radios are typically frequency agile and have intelligence designed to opportunistically and cooperatively share a set of frequency channels that may have primary or priority users, such as UHF television channels. Due to the variety of commercial wireless systems around the world, there are several standardization activities including the International Telecommunication Union, IEEE, European Telecommunications Standards Institute, and European Association for Standardizing Information and Communication Systems.[44] Interestingly, much of the cognitive radio technology is built upon software defined radio technology such as the DARPA Speakeasy program starting in 1990 and was a precursor to the JTRS effort.[45] Cognitive radio capabilities could be used to ease the spectrum management problems on the battlefield by allowing prioritized radios to access the available frequency bands.

There are many key areas that could support hands-free operation such as face recognition, speech understanding, gesture-based inputs, augmented reality, and image analysis that still require further developments before they are ready for extensive military deployments. Both government and commercial R&D is needed in these areas.

---

[42] 3GPP, "Telecommunication management; Self-Organizing Networks (SON); Concepts and requirements R11," 3GPP, TS 32.500, 2012.
[43] ETSI, "Autonomic network engineering for the Self-managing Future Internet: Scenarios, Use Cases, and Requirements for Autonomic/Self-Managing Future Internet," ETSI GS AFI 001 V1.1.1 (2011-06), 2011.
[44] Filin, S., Harada, H., Murakami, H., "International standardization of cognitive radio systems," IEEE Communications Magazine, March , 2011, pp. 82-89.
[45] Lackey, R.I., Upmal, D.W., "Speakeasy: the military software radio," IEEE Communications Magazine, Vol. 33, No. 5, 1995, pp. 56-61.

5.2 Policy and Acquisition Issues

There are many questions to consider about strategies for adoption of commercial technology as the DoD moves forward from the current situation:

- Timing of adoption. When is the appropriate time to adopt a technology? Should DoD only consider products have reached the consumer (mass) market? Should the DoD wait until formal standards have been adopted or risk choosing one of the emerging possible standards? An apparent strategy is to adopt technology that has seen extensive commercial adoption and then use that as a base to customize for DoD use, for example, as with Android-based smartphones and tablets that are being modified.
- Customization. How much can a commercial solution be customized without sacrificing their inherent cost and timeliness benefits? How does the customized product remain up to date with patches and upgrades from the original provider? What is the MOTS architecture?
- Early investment. How can DoD ensure that commercial solutions are able to meet its requirements? Is early investment in R&D sufficient? If not, what incentives—other than traditional program of record acquisitions—can DoD provide to industry?
- Standardization. How much standardization is desirable? Enough to ensure a coherent architecture and routine interoperability. But not enough to stifle innovation.
- Acquisition – Once a COTS candidate has been identified, the DoD must be able to define, procure or initiate the development in a timely manner, understanding that the target device has a lifetime of less than two years.

Another issue is how to incentivize the industry to either incorporate features required or desired by the military into their products. If a feature is dual use then Government R&D can spawn early development but should then hand off to industry and not bog them down with the paperwork. For example, the variants of the JTRS radio that have been developed by industry that are finding a place in the field because they are more capable than the envisioned program of record devices.

6 Conclusion

Several technology, policy, and acquisition trends have come together to 1) increase the availability of viable and cost-effective commercially-based ICT solutions, 2) drive the demand for commercial ICT at the tactical edge, 3) cause the DoD to relax unnecessarily stringent robustness and security constraints, and 4) change the way the DoD acquires and uses ICT.

These trends have enabled the vision of net centric warfare to finally come close to being realized, in large part due to advances in the commercial sector and DoD's move towards an agile acquisition process that enables it to take advantage of commercial innovations in a timely manner. To sustain progress on this path, the DoD should leave design and engineering tradeoffs to industry, and, in keeping with lessons learned from recent experiences, focus its resources on architecture development, research, and integration and test.

Commercial Technologies at the Tactical Edge

18th ICCRTS
June 19, 2013

Jonathan Agre, Karen Gordon, Marius Vassiliou
Institute for Defense Analyses

Overview

- Major trends driving use of COTS
- Challenges of the tactical edge
- Examples of experiments and pilots
- Identification of areas for further R&D
- Policy and Acquisition Issues
- Conclusions

Trends

- Declining influence of the DoD in the ICT sector
- Consumerization of ICT
- Growing demand for cyber security
- Moderation of requirements
- Popular adoption by DoD of telework
- Increasing unsatisfactory outcomes of ICT programs of record

COTS Growth Curves

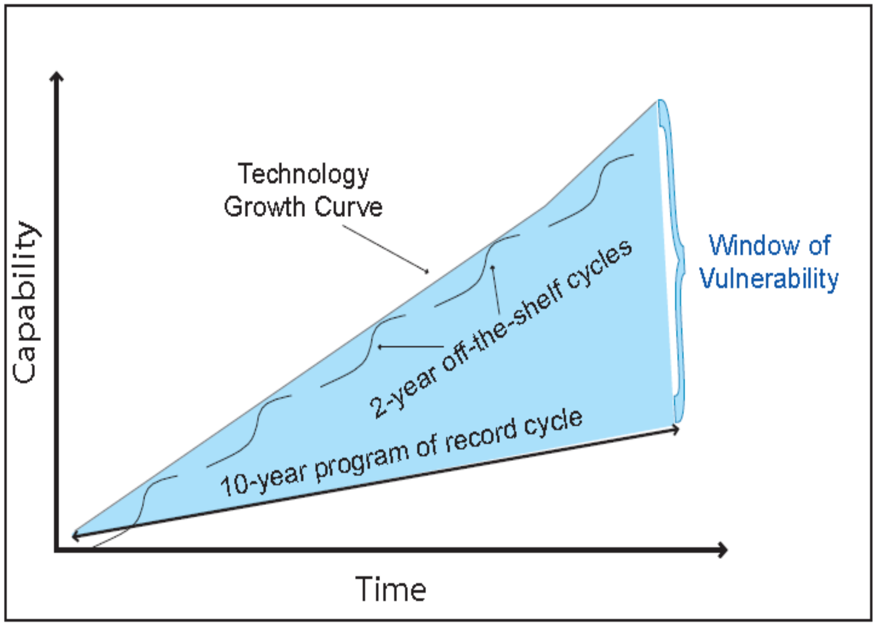


Figure 1

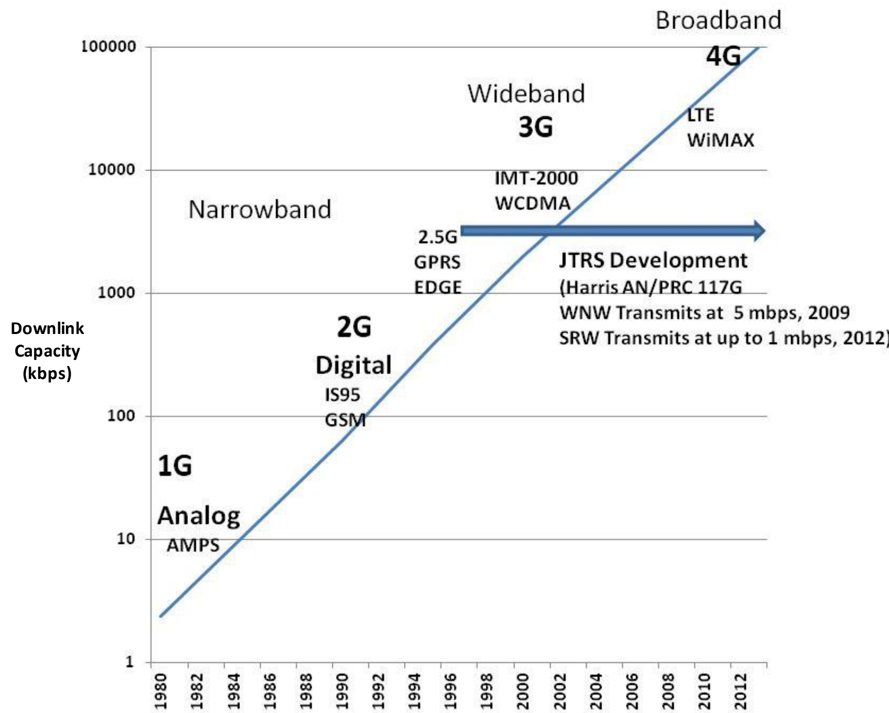
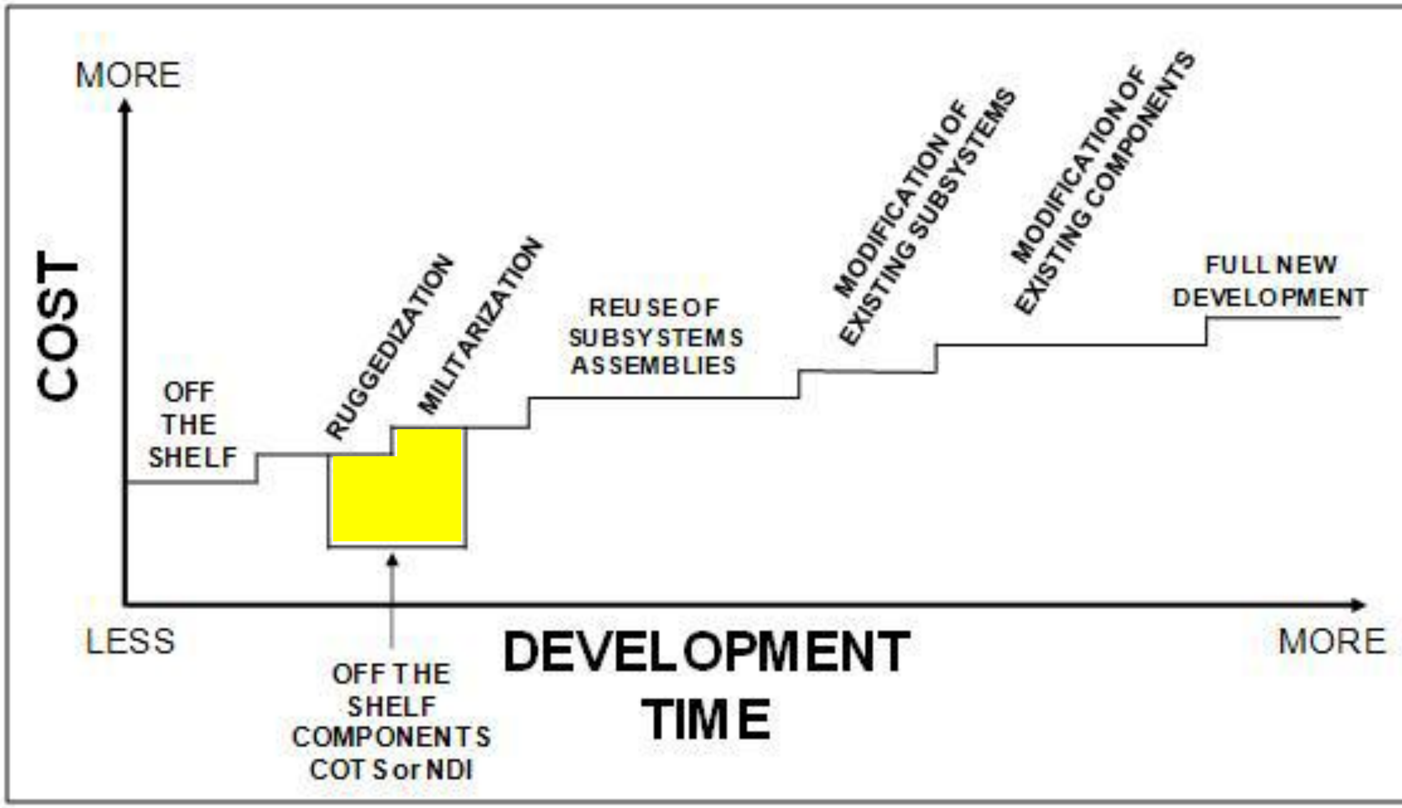


Figure 2

Figure 1 Source: K. J. Cogan and R. De Lucio, *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) During Operation Iraqi Freedom Combat Operations (Mar-Apr 2003),*

Spectrum of Development Strategies



MOTS – Modified-off-the-shelf

Modifications to COTS for military purposes that retains ability to keep up with COTS product evolution

Source: Test & Evaluation Management Guide, Sixth Edition, US DoD, December, 2012, Chap 23

Issues with COTS and the Tactical Edge

Interoperability/Integration	With the IP-based GIG and with existing tactical network equipment – JTRS, WIN-T (JNN) and WIN-T INC 2
Disconnected, Intermittent, and Limited (DIL) Communications	Delay Tolerance
	Mobile Ad Hoc Networks (MANETs)
	Loss of infrastructure
Security	Cyber Offense/Defense methods
	Encryption for data at rest/data in transit
	LPI/LPD, Antijam, Anti-spoof
	Authentication – 2 factor, biometrics
	Cross domain
	Patching
Environmental Factors	Rugged, water proof
	User interface -sun glare, night vision mode, low light, touchable with glove
Acquisition	Supply-chain considerations
Network Operations and Management	Spectrum
	AAA
	Monitoring, Remote auditing
	Loss of infrastructure
	Capture of equipment (remote wipe)
	Remote peripheral control
Size, Weight, and Power (SWAP) Constraints	Power requirements, battery life, battery type
	Portability
App Management	App ecosystem

Hardened Smartphones, Tablets

Sample
Commercial Features

- -Multi-band cellular radio (2G, 3G, 4G, LTE)
- -WiFi (b/g/n), Bluetooth
- -Near Field Communication
- -Microphone
- -High resolution display
- -GPS
- -Accelerometer
- -High resolution Camera
- -Multiprocessors
- -Android OS and Application Ecosystem
- -Voice, Data, Video
- -Internal Storage
- -SIM, SD, MicroSD interfaces
- -USB (or similar) support
- -Stereo Headphone jack

Sample
Military Features

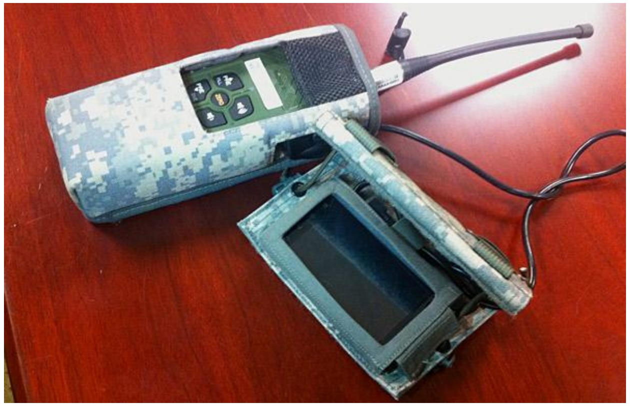
- -Ruggedized
- -Tactical Radio Interface
- -Encryption (e.g., FIPS 140-2, NSA Suite B)
- -CAC Authentication

Sample
Public Safety Features

- -Ruggedized
- -Public Safety band
- -Push to talk

Smartphone Pilots

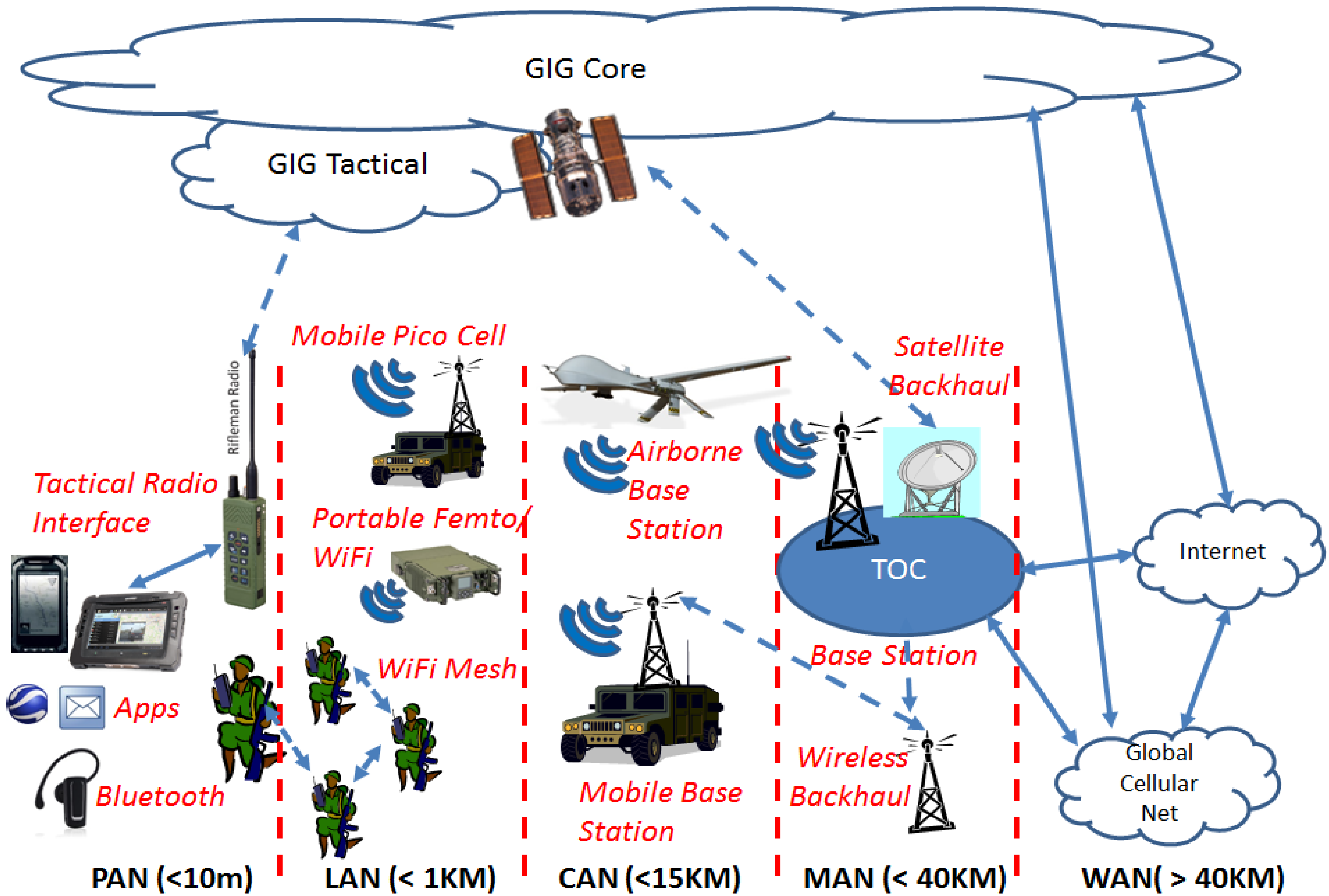
- Nett Warrior – C2 to the foot soldier
  - Ruggedized phone, plugs into AN/PRC154/Rifleman Radio
  - Location information
  - NIE test results highlighted issues
- NSA Fishbowl Project – Provide secure communications over COTS Android phone
  - Mobility Capabilities Package
- USMC Trusted Handheld Platform
  - Virtualization, isolation, HW root of trust, trusted boot
  - Modular development
- Multi-Access Cellular Extension (MACE)
  - RF ranging for location in GPS challenged environments (WiFi/Cellular to WIN-T)



Military Capabilities and Commercial Apps

Military Capability	Similar Commercial Smartphone/Tablet Apps
Command and Control	Chat/IM, SMS, MMS, voice call, video call, Twitter, email, Skype
Mission Planning and Execution	Electronic Flight Bag
Situation Awareness (Blue Force Tracking)	WAZE, Google Maps/Earth, StarChart, Location-based Apps, News feeds
Streaming Video	YouTube, Hulu, Crackle
ISR	Home Monitoring, Friends Tracking, Picture tagging
Soldier as a Sensor	WAZE, Ratings
Biometrics	Face, Voice, Keystroke, IRIS Recognition, fingerprint matching, browsers
Secure, Hands-Free Communications	WICKR, Speech-to-text, Siri
Information Sharing, Access	Dropbox, browsers, Splashtop Whiteboard
Document and Media Exploitation (DOMEX)	Google Translate, iTranslate, Mobile OCR
Education, Training	YouTube, Wikipedia, Dictionary,
Personal applications	Alerts, financial, social media, shopping, games, etc

COTS Comm and Tactical Comm



COTS Networking for the Tactical Edge

- AT&T Remote Mobility Zone – Drop in cellular base station and Satcom for disaster response and remote locations
- KnightHawk (Harris) – Hardened 3G Cellular capability in a box for the field
- Navy Wireless WWAN – 4G LTE cellular net for ship-area network
- Airborne cellular base station
  - BACN (Northrup-Grumman)
  - Forward Airborne Secure Transmission and Communications (FASTCOM)

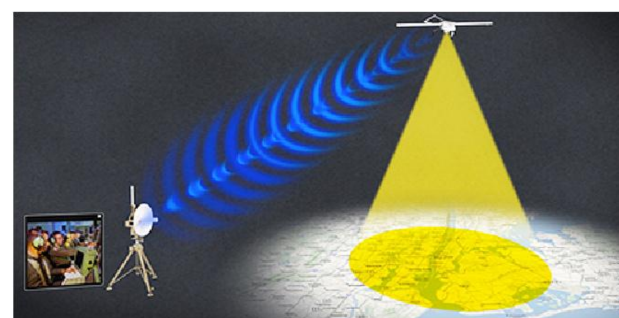


Figure 2 — UAV over New York

Tactical Radio Alternatives to Program of Record

- Mid Tier Vehicular Radio (MNVR) – more affordable alternative to the Ground Mobile Radio
- JTRS Rifleman Radio fair and open competition for full rate production
  - Goal to incorporate state-of-art COTS
- Soldier Radio Waveform (SRW) Appliqué
  - Add an SRW capability to existing vehicle SINGCARS radio
  - Agile bidding process

AN/PRC 152A
(SRW - Harris)

AN/PRC 117G
(MNVR - Harris)

AN/PRC 154 Rifleman radio
(Thales)

RF 330E TR
(Rifleman Radio - Harris)

Selected R&D Areas that can impact Tactical Networks

- Software Defined Networking (SDN)
- Autonomic Networks (ANs)and Self Organizing Networks (SONs)
- Cognitive radio – spectrum sharing
- Hands-free operation
  - Face recognition, gesture-based inputs, speech recognition
- Software engineering methods to address MOTS

Policy and Acquisition Issues/Questions

- Timing of adoption
  - When to adopt in terms of product life-cycle? Does there need to be a mass market?
- Customization
  - How to accomplish MOTS to realize benefits? How to do patches and updates?
- Early investment
  - How to ensure COTS products are available with desired capability?   Is early R&D investment sufficient? How much?
- Standardization
  - Wait for an adopted standard? Emerging standards? Should DoD participate in standards development?
- Acquisition
  - How to efficiently acquire? How can DoD define requirements in a timely manner? How can DoD regulations be simplified for COTS/MOTS
- Incentives
  - How to interest developers in the DoD-size market?

Samsung Evolution Kit TV

Replace modular box to upgrade TV

Conclusions

- Recent trends have come together to:
  - increase the availability of <u>viable</u> and cost-effective commercially-based ICT solutions
  - drive the demand for commercial ICT at the tactical edge,
  - cause the DoD to relax unnecessarily stringent robustness and security constraints,
  - change the way the DoD acquires and uses ICT
- DoD needs to develop strategies and policy to take maximum advantage of the current situation
  - Standardization, MOTS

Opportunities are here to leverage COTS to increasingly realize goals of Net-Centric operations

Commercial Communications in Military Applications

Communication Regime	Commercial Technology	Commercial Examples	Application	User Mobility	Infrastructure Mobility	Military analog /Example/Prototype Adoption
PAN	Bluetooth, NFC	Embedded in smartphone, tablet	Ear-Mic, Headmounts, Authentication	Dismounted		Wired, tethered interfaces CAC smartcard
	GPS	Embedded in smartphone	Location-based applications			PLGR, DAGR
	USB, Sleeves		Interface to Tactical Nets			Intf to Riflemanr Radio, SINCGARs, MONAX
LAN	WiFi APs, MiFi Hotspots, Femto cellular	AT&T Femto cell	Voice, data, video	Dismounted	Fixed or Portable	Knightlite, JTRS Rifleman Radio, SINCGARS
	WiFi Mesh		Voice, data,	Dismounted	Portable	MACE App(Mesh), JTRS Rifleman Radio MANET, Harris 117G
CAN	3G, 4G LTE Mobile Base Station	ATT ARMZ, LGS Pico, Qualcomm,	Voice, data, video, position	Mobile	Portable	KnightHawk, LM MONAX, SRW Appliqué, MNVR
	Airborne Base Station	AirGSM	Voice, data, video	Mobile	Portable	FASTCOM, BACN, LM MONAX
	Backhaul	WiBack, Many Satcom providers	Backhaul for control and data		Fixed, Portable	WIN-T
MAN	3G, 4G-LTE Base Station	Many commercial providers	Voice, data, video, position	Mobile	Fixed or Slowly mobile	Navy WWAN